PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06K 9/00

A1

(11) International Publication Number: WO 97/38392

(43) International Publication Date: 16 October 1997 (16.10.97)

(21) International Application Number: PCT/CA96/00234

(22) International Filing Date: 11 April 1996 (11.04.96)

(71)(72) Applicant and Inventor: DE LANAUZE, Pierre [CA/CA]; 1231 rue Théorêt, Ile Bizard, Quebec H9E 1H7 (CA).

(74) Agents: FORTIN, Jean-Pierre et al.; Swabey Ogilvy Renault, Suite 1600, 1981 McGill College Avenue, Montreal, Quebec H3A 2Y3 (CA).

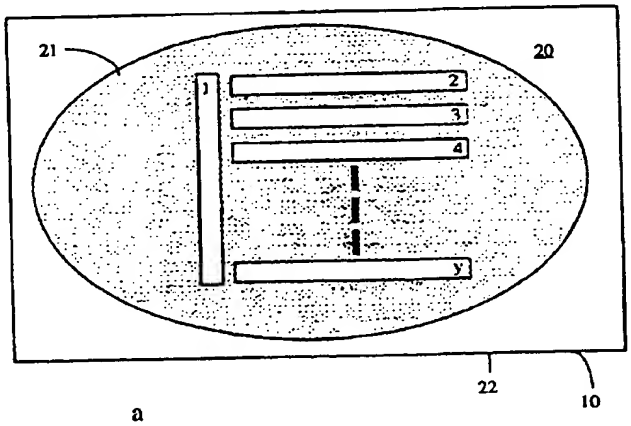
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

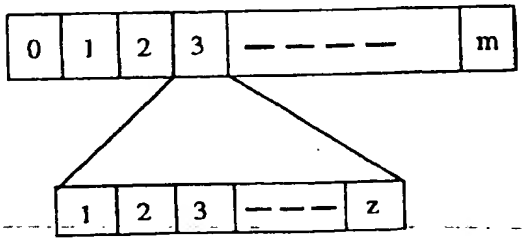
(54) Title: METHOD AND APPARATUS FOR CONFIRMING THE IDENTITY OF AN INDIVIDUAL

(57) Abstract

A method and apparatus, for scanning the fingerprint to confirm the identity of an individual, is disclosed. A scanning surface is used to receive the finger of the individual and to form an optical pattern created at the contact area between the fingerprint of the finger and the scanning surface. The optical pattern is converted to an electrical signal and to n bytes of digital information. A processor then selects y byte sequences, each byte sequence having m bytes, wherein the product of m and y is less than n. The selected byte sequences are stored such that when the byte sequences are detected out of the n bytes, the identity of the individual is confirmed.



a



b

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD AND APPARATUS FOR CONFIRMING THE IDENTITY OF AN INDIVIDUAL

Summary of the Invention

This invention relates to methods and apparatus for identification of individuals, but more particularly to a method and apparatus for confirming the identity of an individual by the scanning of the fingerprint of the individual's finger.

Background of the Invention

The use of an electronic representation of fingerprints for identification purposes has increased substantially in the last few years. This increase is due mainly to the improvements and miniaturizations made in the field of optics and electronics.

Fingerprints are, for example, used in high security establishments for providing or denying access to secure areas. For example, access to certain rooms or areas requiring high levels of security, may require fingerprint identification. Also, with the recent increase in credit card fraud, some credit card suppliers have experimented with intelligent credit cards, wherein fingerprints are used to authenticate the user of the card. An optical fingerprint reader is used during the credit card scanning process to determine whether the individual using the card is the authorized user of the card.

The need for fingerprint identification and authentication has required increasingly accurate fingerprint scanning devices. In some instances, ultrasonic wave and laser scanning techniques have been used to create holographic or 3-dimensional representations

of the fingerprint. Some scanners also make use of special concave scanning surfaces and other scanning techniques to better recreate the scanned image of the fingerprint.

A problem associated with obtaining an accurate representation of a fingerprint is the amount of memory required to store the optical data obtained in the scanning process. Even though that information can generally be stored on a card, the amount of memory required to store sample fingerprints of each user of a banking machine of, say, only one banking institution, would simply be too large to store at each banking machine. For example, if a good monochromatic image is described by 1000 x 1000 pixels and if each pixel is quantized to 256 levels of gray, then 8 million bits will be required to store or transmit such an image. It would take 8 bits per pixel to code the gray-level values of the image.

Another problem associated with the use or storage of fingerprints is with regards to maintaining confidentiality of the stored information. The extreme accuracy provided by some of these scanners has even been criticized. In some cases, objections on privacy grounds have been raised. For example, there is a perception that the use of the data containing an exact replicate of one's fingerprint might be improperly used by a third party.

This concern or fear amongst user groups has of course limited or delayed the introduction of fingerprint scanners or authentication devices for general public use.

Accordingly, there exists a need for an authentication device which can make use of the uniqueness provided by a fingerprint, but wherein the information necessary to authenticate the fingerprint is insufficient to reconstruct or duplicate the entire fingerprint.

Summary of the Invention

It is therefore an object of the present invention to provide an authentication device which can confirm the identity of an individual by using a limited amount of information contained in a fingerprint.

Another object of the present invention is to provide an authentication device in which the information necessary to authenticate the fingerprint is insufficient to reconstruct or duplicate the entire fingerprint.

Another object of the present invention is to minimize the storage required to memorize the information obtained from the scanning of the fingerprint.

According to a first aspect of the invention, there is provided an apparatus for confirming the identity of an individual by the automatic scanning of a fingerprint. It is comprised of a scanning device for scanning the fingerprint of the individual's finger so as to create an optical pattern of the fingerprint of said finger. A conversion circuit is used for converting the optical pattern to an electrical signal and an A/D converter is used for converting the analog electrical signal to digital information. The digital information is comprised of n bytes of digital information. A processor is used for receiving the n bytes of digital information and for selecting a number y of byte sequences, each byte sequence having m bytes, wherein the product of $m \times y < n$. A memory stores the selected byte sequences, such that when the correct byte sequence is detected out of said y byte sequences, authenticity of said individual is determined.

According to another aspect of the invention, there is provided a method confirming the identity of an individual, by scanning the fingerprint of the individual. As a first step, a scanning surface, adapted to receive the finger of said individual, is scanned in order to form an

optical pattern representative of the contact area between the fingerprint of said finger and said scanning surface. Then, the optical pattern is converted to an electrical signal and the electrical signal is converted to n bytes of digital information. Once the n-bytes of digital information are received at a processor, a number y of byte sequences are selected. Each byte sequence has m bytes, wherein the product of m x y < n. A memory containing byte sequences representative of fingerprints of a number of individuals requiring authentication is accessed and a comparison is done to determine whether the byte sequences selected by the processor and the byte sequences stored in the memory are the same, such that authenticity of said individual can be determined.

Description of the Drawings

Figure 1a is a top view of a fingerprint scanning apparatus according to an aspect of the invention;

Figure 1b is a side view illustrating the layout of components which can be used to construct the fingerprint scanning apparatus of Figure 1a;

Figure 2a illustrates the data selection process of the scanned optical pattern according to one embodiment of the invention;

Figure 2b is a representation of a byte sequence selected in the process described in Figure 2a; and

Figure 3 is a block diagram of the scanning apparatus shown in Figure 1b, according to an embodiment of the invention.

Description of the Preferred Embodiment

Referring now to Figure 1a, we have shown a top view of a fingerprint scanning apparatus which can be used

as an embodiment of the present invention. A scanning area depicted by reference numeral 10 is disposed on scanning block 11 which contains the required circuitry to confirm the identity of a user. In Figure 1b we have shown a side, open view of the scanning apparatus, illustrating a general layout of components which can be used for the scanning and authentication process. The scanning area as shown at 10, can either be open directly above the scanning device or include a scanning surface, comprised of a concave surface in the form of a glass plate with a finger size indentation or recess. When a scanning surface is used, a finger 'print' pattern is created by the contact of the finger's papillary lines against the scanning surface. This pattern is scanned to create an optical pattern. When a scanning surface is not used, the scanning device creates an optical pattern which is a representation of the light and dark areas created by the papillary lines of the finger. It will be known to those knowledgeable in the art, that the scanning surface 10 of Figures 1a and 1b is for illustration purposes only. The actual surface used will depend on the application.

The scanning block 11 comprises an optical scanning device in the form of a Charged Coupled Device (CCD) 12. Again, it will be understood by those knowledgeable in the art that other types of image detectors or photo detectors can of course be used. In order to provide sufficient light on the scanning surface, light emitting diodes 13 and 14 can be used. The diodes can emit visible light or light in the infrared end of the spectrum. The advantage of using infrared LEDs, is that no additional light source is required to illuminate the fingerprint. When infrared illumination is used, the CCD 12 is tuned to operate in the infrared end of the light spectrum. The end result is, of course, to provide a

scanning device capable of determining the pattern provided by the capillary lines of the finger.

Other types of scanning devices can also be used. For example, an ultrasonic wave emitter, such as described in US Patent 4,977,601 can provide an enhanced image of the fingerprint.

Once an image or optical pattern representing the fingerprint of the user's finger is obtained, CCD 12 converts the scanned pattern to an electrical signal for further processing by processor 15 and storage at memory 16, as will be described in further detail, below. A lens 17 may be used to focus the fingerprint image on the CCD surface.

Referring now to Figure 2a, there is shown an illustration which can be used to describe the scanning and processing steps used to confirm the identity of an individual. In Figure 2a, reference numeral 20 represents a portion of the scanning surface shown at numeral 10 of Figure 1a. Numeral 21 represents the contact area obtained when a finger is placed on the scanning surface 20. The shaded area thus is a representation of the fingerprint.

With the scanning apparatus of the present invention, the scanning of the fingerprint is completed as described above. That is, the fingerprint is illuminated and an optical pattern detected. However, in the present invention, the resulting image of the fingerprint is processed to eliminate gray areas leaving a high contrast black and white representation of the fingerprint. The fingerprint representation has a lower resolution and thus contains less information to memorize. Also, even though the entire fingerprint pattern 21 is scanned, only a selected portion or portions 22 of the fingerprint pattern is used in the authentication process. Although the size of the selected portions can vary, it was determined that for a fingerprint representation of lower resolution which

is made up of 1 kbyte of data, 100 bytes would be sufficient to identify one individual from millions of other users.

The selected portion 22 is a byte sequence selected according to a predetermined pattern. The byte sequence format is shown in Figure 2b. It is comprised of m bytes, each byte containing z bits of information. Although a byte normally has 8 bits of information, it can consist of any arbitrary number of bits.

The number of byte sequences y is selected such that the total number of bytes selected, i.e.. y x m is less than the total number of bytes n required to reproduce the fingerprint pattern 21. Thus, mathematically, the total number of bytes selected by the processor can be represented by:

i) $y \times m < n$

wherein

y is the number of byte sequences;

m is the number of byte per sequence; and

n is the total number of bytes required to reproduce the fingerprint pattern.

We will now describe the operation of the invention in accordance with the block diagram of Figure 3. When confirmation of a user's identification is required, the user's fingerprint is first scanned by the CCD 30. An analog electrical representation of the fingerprint is obtained at output 31. This signal is of varying frequency and amplitude.

In order to eliminate the gray scale regions contained in the signal, the analog signal is passed through an automatic gain control circuit 32 and a noise filter 34. The output signal 33 is a signal of constant amplitude. The output signal 33 is then filtered by noise

filter 34. The filter's parameters are set according to the specific application and carrier frequency used. In general, any unwanted gray scale region or noise is filtered before the signal is converted in digital form. This way, the gray areas or gray scale regions are filtered from the image to reduce the image's resolution.

In optics, the term resolution is a measure of the ability to delineate picture detail. In a monochromatic image of a face, the use of gray scale regions improves the resolution or quality of the picture. Facial features are easier to detect in a gray scale picture. The presence of these gray regions in the fingerprint pattern would therefore substantially increase the amount of bytes required to authenticate the user's fingerprint.

The principles behind the use of contrast and gray scales are well know to those knowledgeable in the art of video imaging and need not be described further.

The signal 35 at the output of the filter is a high contrast black and white or monochromatic image of the fingerprint.

The output 35 of the filter 34 is then digitized by an analog-to-digital conversion circuit 36. The resulting signal 37 is a low resolution, digital representation of the scanned fingerprint.

The processor 38 is used to select, as explained above, a number of byte sequences from the digitized information. The selection of byte sequences can be set at the factory or determined by the service provider. For example, one banking institution could make use of a specific sequence pattern, such as shown in Figure 2a, for all its customers using automatic teller machines. On the other hand, employees of the banking institution may have a different sequence pattern. Since only a small number of byte sequences, say 10, is used for identification, it is

possible to store the byte sequences of all customers at each automatic teller locations owned by that banking institution, even though thousands of customers may be using this banking service. For example, a 500 megabyte hard disk could contain byte sequences of 5 million users. Therefore, a banking or access card combined with Personal Identification Numbers would not be required for accessing one's personal account.

Thus, when a customer wants to make use of the institution's automatic teller machine anywhere in the country, authentication could be done on site using the customer's pre-memorized byte sequence.

The comparator circuit 39 would in this case be used in conjunction with the memory or storage device 40 to confirm the identity of the user. Thus, if the byte sequence stored in memory 40 contains a high percentage of the bytes scanned by the fingerprint scanning device, the identity of the user is confirmed. The level of accuracy or percentage of bytes identified can be selected according the application.

The application circuit 41 can be any of a number of trigger devices used for accessing a specific product or service. For example, other than automatic teller machines, the application circuit could be a lock arrangement for providing access to a vehicle, secure building or other area requiring the use of a sophisticated lock mechanism.

It will of course be obvious to those knowledgeable in this art that other applications wherein user identification is required can make use of this authentication apparatus and method.

The skilled person will recognize that the invention is in no way limited to the exemplifying embodiment described by way of illustration. Any variant or modification, or any equivalent arrangement, must be

regarded as lying within the scope of the invention, as defined by the following claims.

CLAIMS:

1. An apparatus for confirming the identity of an individual by the automatic scanning of a fingerprint, comprising:

a scanning surface for receiving the finger of said individual;

a scanning device for scanning the scanning surface, such that the pattern created at the contact area between the fingerprint of said finger and said scanning surface can be scanned and converted to an electrical signal;

an A/D converter for converting said electrical signal to digital information, said digital information comprising n bytes of digital information;

a processor for receiving said n bytes of digital information and for selecting a number y of byte sequences, each byte sequence having m bytes, wherein the product of m and y is less than n; and

a memory for storing the selected byte sequences, such that when said byte sequences are detected out of said n bytes, the identity of said individual is confirmed.

2. An apparatus as defined in claim 1, further comprising a signal processing circuit to deduce the resolution of the electrical signal.

3. An apparatus as defined in claim 2, wherein said signal processing circuit comprises a filter for filtering portions of said signal representing gray scale regions.

4. An apparatus as defined in claim 3, wherein said scanning device comprises a charged coupled device.

5. An apparatus as defined in claim 4, wherein said charged coupled device operates in the infrared region.

BEST AVAILABLE COPY

6. An apparatus for confirming the identity of an individual by the automatic scanning of a fingerprint, comprising:

a scanning device for scanning the fingerprint of the individual's finger so as to create a pattern of the fingerprint of said finger;

a conversion circuit for converting said pattern to an electrical signal;

an A/D converter for converting said electrical signal to digital information, said digital information comprising n bytes of digital information;

a processor for receiving said n bytes of digital information and for selecting a number y of byte sequences, each byte sequence having m bytes, wherein the product of m and y is less than n; and

a memory for storing the selected byte sequences, such that when said byte sequences are detected out of said n bytes, the identity of said individual is confirmed.

7. An apparatus as defined in claim 6, further comprising a signal processing circuit to deduce the resolution of the electrical signal.

8. An apparatus as defined in claim 7, wherein said signal processing circuit comprises a filter for filtering portions of said signal representing gray scale regions.

9. An apparatus as defined in claim 8, wherein said scanning device comprises a charged coupled device.

10. An apparatus as defined in claim 9, wherein said charged coupled device operates in the infrared region.

11. A method of automatically scanning the fingerprint to confirm the identity of an individual, comprising the steps of:

scanning a surface adapted to receive the finger of said individual so as to form an optical pattern created at the contact area between the fingerprint of said finger and said scanning surface;

converting said optical pattern to an electrical signal;

converting said electrical signal to digital information, said digital information comprising n bytes of digital information;

receiving said n bytes of digital information at a processor;

selecting a number y of byte sequences, each byte sequence having m bytes, wherein the product of m and y is less than n; and

storing said selected byte sequences such that when said byte sequences are detected out of said n bytes, the identity of said individual is confirmed.

12. A method as defined in claim 11, further comprising the step of filtering said electrical signal to eliminate portions of the signal representing gray scale regions.

13. A method as defined in claim 12, wherein said surface is scanned using infrared light.

14. A method as defined in claim 13, wherein said optical pattern is converted to an electrical signal using a charged coupled device.

15. A method of confirming the identity of an individual, by scanning the fingerprint of the individual's finger, comprising the steps of:

scanning the fingerprint side of said individual's finger so as to form an optical pattern;

converting said optical pattern to an electrical signal;

converting said electrical signal to digital information, said digital information comprising n bytes of digital information;

receiving said n bytes of digital information at a processor;

selecting a number y of byte sequences, each byte sequence having m bytes, wherein the product of m and y is less than n;

accessing a memory containing a number of byte sequences representative of fingerprints of a number of individuals requiring identity confirmation; and

comparing the byte sequences selected by said processor and the byte sequences stored in said memory such that when a percentage of said selected byte sequences are detected in said memory, the identity of said individual is confirmed.

16. A method as defined in claim 15, further comprising the step of filtering said electrical signal to eliminate portions of the signal representing gray scale regions.

17. A method as defined in claim 16, wherein said surface is scanned using infrared light.

18. A method as defined in claim 17, wherein said optical pattern is converted to an electrical signal using a charged coupled device.

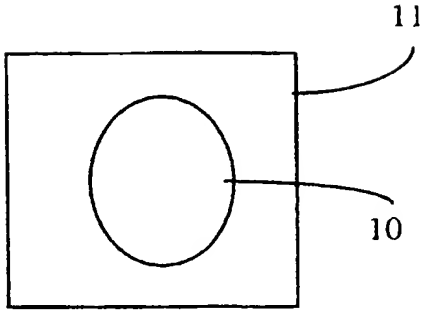


Figure 1a

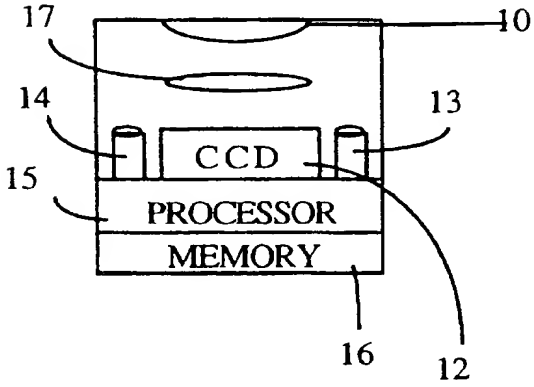


Figure 1b

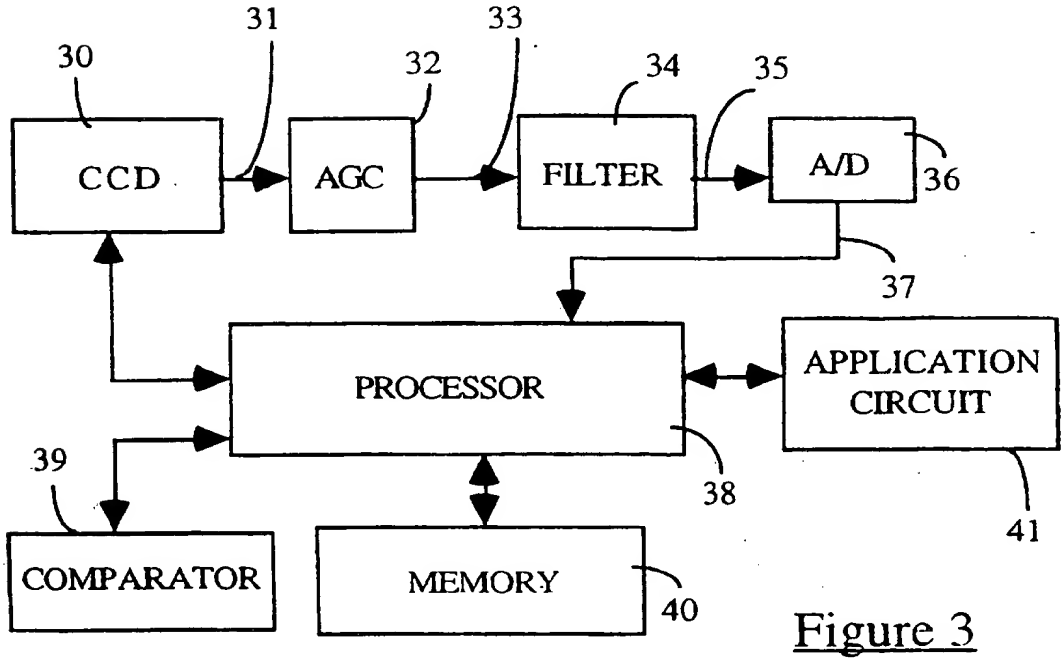


Figure 3

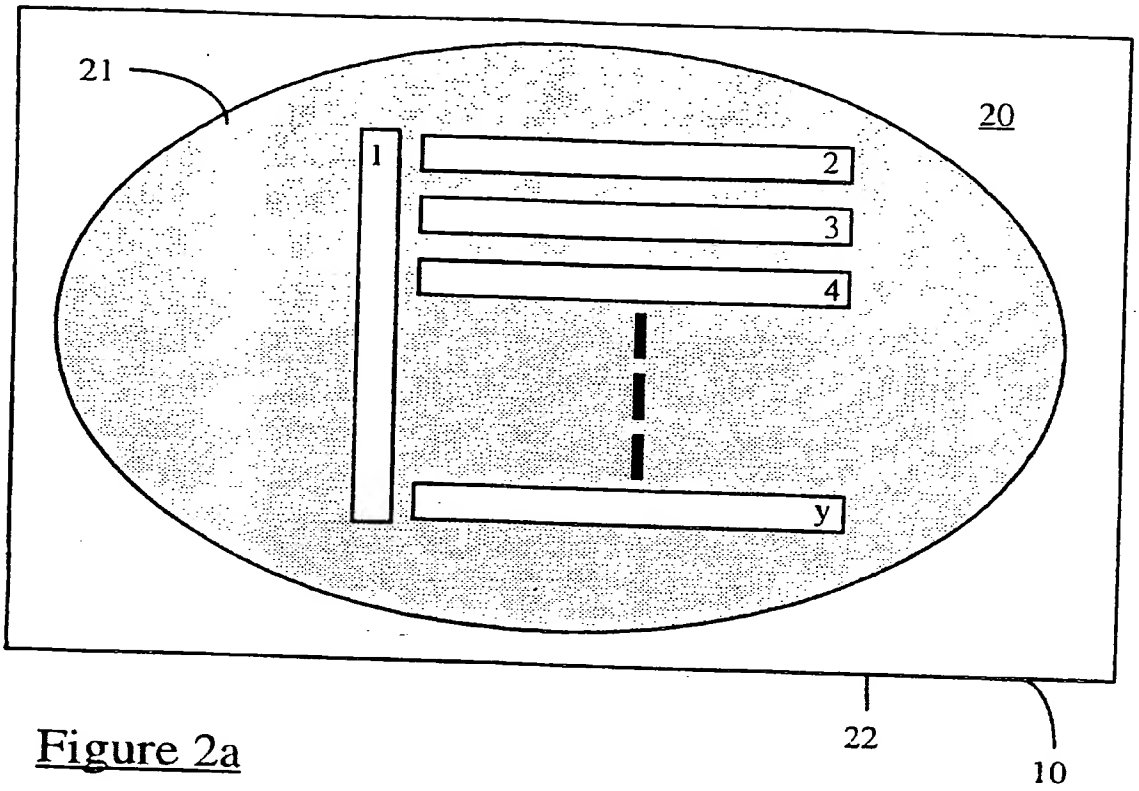


Figure 2a

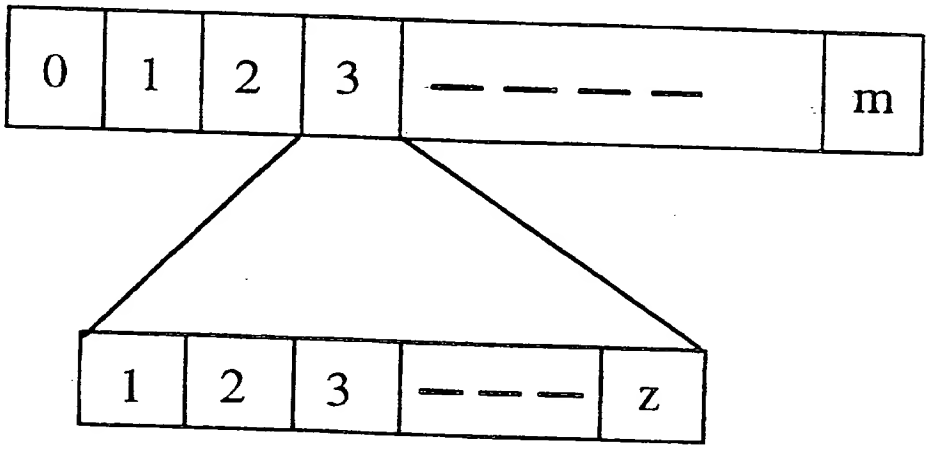


Figure 2b

INTERNATIONAL SEARCH REPORT

Inter ial Application No
PCT/CA 96/00234

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06K9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TECHNOLOGIES TODAY AND TOMORROW, NEW ORLEANS, APRIL 1 - 4, 1990, vol. 1 OF 3, 1 April 1990, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 343-347, XP000203123 HIRONORI YAHAGI ET AL: "MOVING-WINDOW ALGORITHM FOR FAST FINGERPRINT VERIFICATION" see the whole document ---	1,6,11, 15
X	EP,A,0 251 504 (IDENTIX INC) 7 January 1988 see column 4, line 28 - line 39; figures 6-8 --- -/--	1,3,4,6, 8,9,11, 12, 14-16,18

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 November 1996	10.12.96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Granger, B

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte mal Application No
PCT/CA 96/00234

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PROC. IEEE 1991 CUSTOM INTEGRATED CIRCUITS CONF., 12 May 1991, SAN DIEGO, CA, USA, pages 12.1.1-12.1.4, XP000295730 S. ANDERSON ET AL: "A single chip sensor & image processor for fingerprint verification" see figure 1 ---	4,9,14, 18
A	EP,A,0 640 933 (GIM GES FUER INNOVATION UND MA) 1 March 1995 see column 3, line 42-55; figure 1 -----	5,10,13, 17

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inu onal Application No
PCT/CA 96/00234

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0251504	07-01-88	US-A-	5067162	19-11-91
		DE-D-	3788085	16-12-93
		DE-T-	3788085	03-03-94
		JP-A-	63041989	23-02-88
EP-A-0640933	01-03-95	DE-A-	4429829	02-03-95